netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 28

July 20, 2007

Table of Contents

Product Focus

Apache Chunked Vulnerability Scanner – The Apache Chunked Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Apache Chunked Encoding buffer overflow.

This Week in Review

Bruce Schneier on 'The Psychology of Security'.Austrialians willing to pay for extended airport security. How do the FEDs look at identity theft? When your laptop gets stolen.

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

❖ **BT Counterpane’s founder and chief technology officer talks to SA Mathieson at Infosecurity Europe**

Interview: Bruce Schneier
Bruce Schneier packed out the show's keynote theatre when he spoke about 'The Psychology of Security', based on a draft essay he published in February. He outlined a range of research suggesting that our perceptions of a given risk are heightened if it is - among other things - spectacular, discussed widely, outside our normal

experience or willingly taken rather than beyond our control. Such biases are ideal for hunter-gatherers living in small family groups in Kenya in 100 000BC, he argues, but not for modern life.

So how does this apply to infosecurity risks? "The obvious place is the people who are afraid of cyber-terrorism, while minimising cyber-crime," he says. "Cyber-terrorism gets the news, it's the hot topic, it's the scary topic and people are afraid of it. Cyber-crime doesn't get as much news, and I think people very much underplay that threat. You see it also when people overplay the threat of peer-to-peer, or they get all scared of people bringing their iPods in and maybe putting data on it. They forget that data could walk out on paper. So there is a lot of people reacting to the news, instead of to the reality of security. Now, it's hard to blame them. This is what's reported, this is what people worry about, but I think there's a big difference in how people perceive internet security and what's really going on.

Infosecurity

Full Story :
http://www.infosecurity-magazine.com/features/mayjune07/interview_schneier.html

❖ Travellers happy with bio checks

AUSTRALIANS appear happy to accept and pay for additional security at airports provided it keeps them safe or allows them to get through more quickly.
Research by technology firm Unisys shows 98 per cent of Australians are prepared to use a photograph to establish their identity, while three in four are happy to have their fingerprints taken and 69 per cent would agree to iris scans.

Unisys found more than half of domestic travellers would be prepared to pay a higher ticket price if it produced tangible security improvements, and 71 per cent would be prepared to provide biometric data to airlines.

The technology company, which is helping develop facial recognition and fingerprint technology for border security in Australia, believes the acceptance of the increased security measures means it will only be a matter of time before there is a registered traveller scheme in Australia.

Austrialian IT

Full Story :
http://www.australianit.news.com.au/story/0,24897,22102544-5013044,00.html

❖ Identity theft? What identity theft?

GAO report concludes that theft of personal information isn't a problem, but notifying consumers Is
The GAO reports that identity theft really isn't a problem. The problem, apparently, is that the process of notifying consumers whenever their personal financial information has been compromised is confusing us simple-minded folks.

Yes, I've got that right. It's not a comedic headline from The Onion.

The SANS NewsBites, one of my top information sources on security news, turned me on to The United States Government Accountability Office's new report to congressional requesters called Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown. The 50-page report was developed to assist Congress with crafting all the various data breach notification legislation being proposed (the Data Security Act of 2007 (H.R. 1685), Data Accountability and Trust Act (H.R. 958), Identity Theft Prevention Act (S. 1178), and the Personal Data Privacy and Security Act of 2007 (S. 495), to name a few.) Overall, it's not an entirely bad report, but it comes to nebulous conclusions.

infoworld

Full Story :
http://www.infoworld.com/article/07/07/20/29OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/07/20/29OPsecadvise_1.html

- **5 Essential laptop security tips**

Laptop theft is a huge problem. It is common nowadays to use a laptop to get work done away from your home or office. Unfortunately, the mobility and technology that make laptops so valuable also make them the target for theft around the world.

If your laptop is stolen, company information can be exposed, as well as your personal information can lead to identity theft. In this hack, we'll show you 5 essential tips to learn how you can keep your laptop more secure.

Tip #1: Never leave any passwords in your laptop case. If you do keep your passwords with your laptop, it's much like keeping the keys in your car. Remember that without your passwords, it will be more difficult to unlock your computer and access your personal information.

Security hacks

Full Story :
http://www.security-hacks.com/2007/07/10/5-essential-laptop-security-tips

New Vulnerabilities Tested in SecureScout

- **13551 Oracle Database Server - Oracle Text component buffer overflow Vulnerability (jul-2007/DB09)**

A buffer overflow vulnerability exists in Oracle Database Server Oracle Text component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Low**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3853

❖ 13550 Oracle Database Server - Oracle Text component buffer overflow Vulnerability (jul-2007/DB08)

A buffer overflow vulnerability exists in Oracle Database Server Oracle Text component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Low**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3857

❖ 13549 Oracle Database Server - Oracle Text component buffer overflow Vulnerability (jul-2007/DB07)

A buffer overflow vulnerability exists in Oracle Database Server Oracle Text component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Low**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3857

- **13548 Oracle Database Server - Oracle Text component buffer overflow Vulnerability (jul-2007/DB06)**

A buffer overflow vulnerability exists in Oracle Database Server Oracle Text component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Low**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3857

- **13547 Oracle Database Server - Oracle Text component buffer overflow Vulnerability (jul-2007/DB05)**

A buffer overflow vulnerability exists in Oracle Database Server Oracle Text component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Low**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:

http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3857

❖ 13546 Oracle Database Server - Oracle Data Mining component buffer overflow Vulnerability (jul-2007/DB04)

A buffer overflow vulnerability exists in Oracle Database Server Oracle Data Mining component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Gather Info** Risk: **Low**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3856

❖ 13545 Oracle Database Server - DataGuard component buffer overflow Vulnerability (jul-2007/DB03)

A buffer overflow vulnerability exists in Oracle Database Server DataGuard component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Low**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3855

❖ 13544 Oracle Database Server - Advanced Queuing component buffer overflow Vulnerability (jul-2007/DB02)

A buffer overflow vulnerability exists in Oracle Database Server Advanced Queuing component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Low**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_prvtaqis.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3854

❖ 13543 Oracle Database Server - JavaVM component buffer overflow Vulnerability (jul-2007/DB01)

A buffer overflow vulnerability exists in Oracle Database Server JavaVM component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Medium**

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* SECUNIA: 26114
http://secunia.com/advisories/26114

CVE Reference: CVE-2007-3853

❖ 16557 Microsoft Windows Vista Firewall Blocking Rule Information Disclosure Vulnerability (MS07-038/935807) (Remote File Checking)

There is an information disclosure vulnerability in Windows Vista that could allow a remote anonymous attacker to send inbound network traffic to the affected system. It would be possible for the attacker to gain information about the system over the network.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Low**

References:

* MS: MS07-038
http://www.microsoft.com/technet/security/Bulletin/MS07-038.mspx
* BUGTRAQ: 20070709 SYMSA-2007-005: Vista Windows Firewall Incorrectly Applies Filtering to Teredo Interface
http://www.securityfocus.com/archive/1/archive/1/473294/100/0/threaded
* CONFIRM:
http://www.symantec.com/content/en/us/enterprise/research/SYMSA-2007-005.txt
* CERT-VN: VU#101321
http://www.kb.cert.org/vuls/id/101321
* BID: 24779
http://www.securityfocus.com/bid/24779
* FRSIRT: ADV-2007-2480
http://www.frsirt.com/english/advisories/2007/2480
* SECTRACK: 1018354
http://www.securitytracker.com/id?1018354
* SECUNIA: 26001
http://secunia.com/advisories/26001
* XF: win-vista-firewall-information-disclosure(35322)
http://xforce.iss.net/xforce/xfdb/35322

CVE Reference: CVE-2007-3038

New Vulnerabilities found this Week

Oracle Products Multiple Vulnerabilities

“SQL injection attacks; DoS (Denial of Service); Buffer overflows”

Multiple vulnerabilities have been reported for various Oracle products. Some of these have unknown impacts, while others can be exploited to bypass certain security restrictions and conduct SQL injection attacks, cause a DoS (Denial of Service), and potentially compromise a vulnerable system.

References:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html

Mozilla Firefox Multiple Vulnerabilities

“Memory corruption; Execute arbitrary code”

Some vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to conduct spoofing and cross-site scripting attacks and potentially to compromise a user's system.

1) Various errors in the browser engine can be exploited to cause memory corruption and potentially to execute arbitrary code.

2) Various errors in the Javascript engine can be exploited to cause memory corruption and potentially to execute arbitrary code.

3) An error in the "addEventListener" and "setTimeout" methods can be exploited to inject script into another site's context, circumventing the browser's same-origin policy.

4) An error in the cross-domain handling can be exploited to inject arbitrary HTML and script code in a sub-frame of another web site.

5) An unspecified error in the handling of elements outside of documents allows an attacker to call an event handler and execute arbitrary code with chrome privileges.

6) An unspecified error in the handling of "XPCNativeWrapper" can lead to execution of user-supplied code.

References:
http://www.mozilla.org/security/announce/2007/mfsa2007-18.html
http://www.mozilla.org/security/announce/2007/mfsa2007-19.html
http://www.mozilla.org/security/announce/2007/mfsa2007-20.html
http://www.mozilla.org/security/announce/2007/mfsa2007-21.html
http://www.mozilla.org/security/announce/2007/mfsa2007-25.html

tcpdump print-bgp.c Buffer Overflow Vulnerability

“Execution of arbitrary code.”

mu-b has reported a vulnerability in tcpdump, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to the incorrect use of the return value of "snprintf()" in print-bgp.c. This can be exploited to cause a buffer overflow by sending specially crafted BGP packets.

Successful exploitation may allow the execution of arbitrary code.

The vulnerability is reported in version 3.9.6. Other versions may also be affected.

References:
http://www.digit-labs.org/files/exploits/private/tcpdump-bgp.c

Yahoo! Messenger Long Email Address Book Buffer Overflow

“Execution of arbitrary code”

Rajesh Sethumadhavan has reported a vulnerability in Yahoo! Messenger, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the processing of address book entries and can be exploited to cause a buffer overflow when a user performs a mouse-over on a contact on the address book with an overly-long email address.

Successful exploitation allows execution of arbitrary code, but requires that the target user is e.g. tricked into accepting malicious contact details.

The vulnerability is reported in version 8.1. Other versions may also be affected.

References:
http://www.xdisclose.com/advisory/XD100002.html

Asterisk Multiple Vulnerabilities

"Denial of Service"

Some vulnerabilities have been reported in Asterisk, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

1) A boundary error exists in the Asterisk STUN implementation, which can be exploited to cause the application to crash via specially crafted RTP packets.

Successful exploitation requires that the chan_sip, chan_gtalk, chan_jingle, chan_h323, chan_mgcp, or chan_skinny is enabled.

2) A boundary error exists in the Asterisk Skinny channel driver (chan_skinny), which can be exploited to cause the application to crash via packets that contain a size field smaller than the actual size of the packet.

Successful exploitation requires that chan_skinny is enabled.

3) A NULL-pointer dereference error exists in the Asterisk IAX2 channel driver (chan_iax2), which can be exploited to cause a DoS via specially crafted LGRQ and LAGRP frames.

Successful exploitation requires that chan_iax is enabled.

4) A boundary error exists in the Asterisk IAX2 channel driver (chan_iax2) within the handling of RTP frames. This can be exploited to cause a stack-based buffer overflow by sending large data payloads (more than 4096 bytes) in a voice or video frame.

Successful exploitation of this vulnerability allows execution of arbitrary code, but requires that the system is configured to connect channels that use RTP and IAX channels.

References:
http://ftp.digium.com/pub/asa/ASA-2007-017.pdf
http://ftp.digium.com/pub/asa/ASA-2007-016.pdf
http://ftp.digium.com/pub/asa/ASA-2007-015.pdf
http://ftp.digium.com/pub/asa/ASA-2007-014.pdf

Trillian "aim://" URI Handler Two Vulnerabilities

"execution of arbitrary code"

Two vulnerabilities have been discovered in Trillian, which can be exploited by malicious people to compromise a user's system.

1) The aim:// URI handler does not verify certain parts of the "aim://" URI before writing it

into a file specified via the unverified "ini=" parameter. This can be exploited to e.g. write a batch file into the Windows "Startup" folder that starts an attacker-defined application by tricking a user into following a specially crafted "aim://" URI.

2) A boundary error within the processing of "aim://" URIs exists in the aim.dll plugin. This can be exploited to cause a buffer overflow by e.g. tricking a user into following a specially crafted "aim://" URI.

Successful exploitation allows the execution of arbitrary code.

The vulnerabilities are confirmed in Trillian Basic 3.1.6.0. Other versions may also be affected.

References:
http://www.xs-sniper.com/nmcfeters/Cross-App-Scripting-2.html

Vulnerability Resource

Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the ‘security portal for information system security professionals’ is well founded. http://www.infosyssec.org/infosyssec/

Thank You

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com.

About SecureScout

SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.
SecureScout is a trademark of NexantiS Corporation.
netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:

Customers in America and Northern Europe contact us at info@netVigilance.com
Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net